Europäisches Patentamt
European Patent Office
Office européen des brevets

Bescheinigung Certificate Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

99480119.9

CERTIFIED COPY OF PRIORITY DOCUMENT

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

I.L.C. HATTEN-HECKMAN

DEN HAAG, DEN
THE HAGUE, 05/01/00
LA HAYE, LE

THIS PAGE BLANK (USPTO)

Europäisches Patentamt
European Patent Office
Office européen des brevets

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.:
Application no.:
Demande n°: 99480119.9

Anmeldetag:
Date of filing:
Date de dépôt: 25/11/99

Anmelder:
Applicant(s):
Demandeur(s):
INTERNATIONAL BUSINESS MACHINES CORPORATION
Armonk, NY 10504
UNITED STATES OF AMERICA

Bezeichnung der Erfindung:
Title of the invention:
Titre de l'invention:
Method and system for detecting and neutralizing unauthorized dynamic host configuration protocol (DHCP) servers in an internet protocol (IP) network

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat: State: Pays:	Tag: Date: Date:	Aktenzeichen: File no. Numéro de dépôt:

Internationale Patentklassifikation:
International Patent classification:
Classification internationale des brevets:
/

Am Anmeldetag benannte Vertragstaaten:
Contracting states designated at date of filing: AT/BE/CH/CY/DE/DK/ES/FI/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE
Etats contractants désignés lors du depôt:

Bemerkungen:
Remarks:
Remarques:

METHOD AND SYSTEM FOR DETECTING AND NEUTRALIZING UNAUTHORIZED DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) SERVERS IN AN INTERNET PROTOCOL (IP) NETWORK

Technical field of the invention

The present invention relates to computer networks, and more particularly to a method and system in an Internet Protocol (IP) network for detecting and neutralizing one or a plurality of unauthorized Dynamic Host Configuration Protocol (DHCP) servers.

Background art

INTERNET

Internet is a global network of computers and computers networks (the "Net"). The Internet connects computers that use a variety of different operating systems or languages, including UNIX, DOS, Windows, Macintosh, and others. To facilitate and allow the communication among these various systems and languages, the Internet uses a language referred to as TCP/IP ("Transmission Control Protocol/Internet Protocol"). TCP/IP protocol supports three basic applications on the Internet:

- transmitting and receiving electronic mail,
- logging into remote computers (the "Telnet"), and
- transferring files and programs from one computer to another ("FTP" or "File Transfer Protocol").

One of the object of TCP/IP is to interconnect networks and to provide an universal communication services: an inter-network, or Internet. Each physical network has its own technology-dependent communication interface, in the form of a programming interface that provides basic communication functions (primitives). Communication services are provided by a software that runs between the physical network and user applications. This software provides a common interface for these applications, independent of the underlying physical network. The architecture of the physical networks is hidden from the user.

The Internet protocol is still evolving through the mechanism of Request For Comments (RFC). New protocols (mostly application protocols) are designed and implemented by researchers. They are brought to the attention of the Internet community in the form of an Internet Draft (ID). The largest source of IDs is the Internet Engineering Task Force (IETF).

IP ADDRESSES

To interconnect two networks, a computer system able to forward packets from one network to the other is attached to both networks. Such a machine is called a router. The term "IP router" is also used because the routing function is part of the IP layer of the TCP/IP protocol.

IP addresses are used by the IP protocol to uniquely identify a host on the Internet (Strictly speaking, an IP address identifies an interface that is capable of sending and

receiving IP datagrams, and one system can have multiple such interfaces. However, both hosts and routers must have at least one IP address, so this simplified definition is acceptable). IP datagrams (the basic data packets exchanged between hosts) are transmitted by a physical network attached to the host and each IP datagram contains a source IP address and a destination IP address.

IP addresses are represented by a 32-bit unsigned binary value which is usually expressed in a dotted decimal format. For example, 9.167.5.8 is a valid Internet address. The numeric form is used by the IP software. The mapping between the IP address and an easier-to-read symbolic name, for example myhost.ibm.com, is done by the Domain Name System

IP SUBNETS

Due to the explosive growth of the Internet, the principle of assigned IP addresses is not flexible enough to allow easy changes to local network configurations. Those changes might occur when:

- A new type of physical network is installed at a location.
- The growing number of hosts requires to split the local network into two or more separate networks.
- Growing distances require to divide a network into smaller networks, with gateways between them.

To avoid having to request additional IP network addresses in these cases, the concept of subnets has been introduced. The assignment of subnets can be done locally, as the whole network still appears to be one IP network to the outside world. The host number part of the IP address is subdivided again into a network number and a host number. This second network is termed "subnetwork" or "subnet". The main

network now comprises a plurality of subnets and the IP address is interpreted as:

<network number><subnet number><host number>

The combination of the subnet number and the host number is often termed "local address" or "local part". Subnetting is implemented in a way that is transparent to remote networks. A host within a network that has subnets is aware of the subnetting but a host in a different network is not; it still regards the local part of the IP address as a host number.

The division of the local part of the IP address into subnet number and host number parts can be chosen freely by the local administrator; any bits in the local part can be used to form the subnet. The division is done using a subnet mask which is a 32 bit number. Zero bits in the subnet mask indicate bit positions ascribed to the host number, and ones indicate bit positions ascribed to the subnet number. The bit positions in the subnet mask belonging to the network number are set to ones but are not used. Subnet masks are usually written in dotted decimal form, like IP addresses.

WORLD WIDE WEB

With the increasing size and complexity of the Internet, tools have been developed to help find information on the network, often called navigators or navigation systems. Navigation systems that have been developed include standards such as Archie, Gopher and WAIS. The World Wide Web ("WWW" or "the Web") is a recent superior navigation system. The Web is :

- an Internet-based navigation system,

- an information distribution and management system for the Internet, and
- a dynamic format for communicating on the Web.

The Web seamlessly, for the use, integrates format of information, including still images, text, audio and video. A user on the Web using a graphical user interface ("GUI", pronounced "gooey") may transparently communicate with different host computers on the system, and different system applications (including FTP and Telnet), and different information formats for files and documents including, for example, text, sound and graphics.

UNIFORM RESOURCE LOCATORS

A resource of the Internet is unambiguously identified by a Uniform Resource Locator (URL), which is a pointer to a particular resource at a particular location. A URL specifies the protocol used to access a server (e.g. HTTP, FTP,..), the name of the server, and the location of a file on that server.

HYPER TEXT TRANSFER PROTOCOL

Each Web page that appears on client monitors of the Web may appear as a complex document that integrates, for example, text, images, sounds and animation. Each such page may also contain hyperlinks to other Web documents so that a user at a client computer using a mouse may click on icons and may activate hyperlink jumps to a new page (which is a graphical representation of another document file) on the same or a different Web server.

A Web server is a software program on a Web host computer that answers requests from Web clients, typically over the Internet. All Web use a language or protocol to communicate with Web clients which is called Hyper Text Transfer Protocol ("HTTP"). All types of data can be exchanged among Web servers

and clients using this protocol, including Hyper Text Markup Language ("HTML"), graphics, sound and video. HTML describes the layout, contents and hyperlinks of the documents and pages. Web clients when browsing :

- convert user specified commands into HTTP GET requests,
- connect to the appropriate Web server to get information, and
- wait for a response. The response from the server can be the requested document or an error message.

After the document or an error message is returned, the connection between the Web client and the Web server is closed.

First version of HTTP is a stateless protocol. That is with HTTP, there is no continuous connection between each client and each server. The Web client using HTTP receives a response as HTML data or other data. This description applies to version 1.0 of HTTP protocol, while the new version 1.1 break this barrier of stateless protocol by keeping the connection between the server and client alive under certain conditions.

DOMAIN NAMES

The host or computer names (like www.entreprise.com) are translated into numeric Internet addresses (like 194.56.78.3), and vice versa, by using a method called DNS ("Domain Name Service"). DNS is supported by network-resident servers, also known as domain name servers or DNS servers.

DYNAMIC IP

There are generally three pieces of information needed by a system to communicate on a TCP/IP network:

- an IP address (to uniquely identify the system on the network),
- a subnet mask (to determine the network and subnet parts of the address), and
- the address of at least one router (if the system is able to communicate with other devices outside its immediate subnet).

These three values represent the bare minimum of information that must be programmed into each device for participating in the TCP/IP world. Often the number of necessary parameters will be much higher. With the exponential growth rate of networking today, it is easy to see that manual programming of these values into every device to attach to the network represents a major administrative workload.

The increasingly mobile nature of the end users also raises problems with regard to configuration of network devices. It is possible to allocate multiple sets of configuration parameters to a device, but:

- this obviously means even more workload for the administrator,
- this is wasteful with respect to the number of IP addresses allocated.

Several components of TCP/IP can automate device configuration, reduce the number of IP addresses allocated, and/or cope with the demands of mobile users.

BOOTSTRAP PROTOCOL (BOOTP)

The BOOTP protocol was originally developed as a mechanism to enable diskless hosts to be remotely booted over

a network as workstations, routers, terminal concentrators and so on. It allows a minimum IP protocol stack with no configuration information to obtain enough information to begin the process of downloading the necessary boot code. BOOTP does not define how the downloading is done, but this process typically uses TFTP "Trivial File Transfer Protocol (TFTP)" as described in *RFC 906 - Bootstrap Loading Using TFTP*. Although still widely for this purpose by diskless hosts, BOOTP is also commonly used solely as a mechanism to deliver configuration information to a client that has not been manually configured. The BOOTP process involves the following steps:

- 1. The client determines its own hardware address; this is normally in a ROM (Read Only Memory) on the hardware.

- 2. A BOOTP client sends its hardware address in a UDP (User Datagram Protocol) datagram to the server. If the client knows its IP address and/or the address of the server, it should use them, but in general BOOTP clients have no IP configuration data at all. If the client does not know its own IP address, it uses 0.0.0.0. If the client does not know the server's IP address, it uses the limited broadcast address (255.255.255.255). The UDP port number is 67.

- 3. The server receives the datagram and looks up the hardware address of the client in its configuration file, which contains the client's IP address. The server fills in the remaining fields in the UDP datagram and returns it to the client using UDP port 68.

- 4. When it receives the reply, the BOOTP client will record its own IP address and begin the bootstrap process.

BOOTP is a draft standard protocol. Its status is recommended. The BOOTP specifications can be found in *RFC 951 – Bootstrap Protocol*. There are also updates to BOOTP, some relating to inter operability with DHCP (Dynamic Host Configuration Protocol), described in *RFC 1542 – Clarifications and Extensions for the Bootstrap Protocol,* which updates *RFC 951 and RFC 2132 – DHCP Options and BOOTP Vendor Extensions.*

DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

The Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the BOOTP protocol, adding the capability of automatic allocation of reusable network addresses and additional configuration options. DHCP messages use UDP port 67, the BOOTP server's well-known port and UDP port 68, the BOOTP client's well-known port. DHCP consists of two components:

- 1. A protocol that delivers host-specific configuration parameters from a DHCP Server to a host.
- 2. A mechanism for the allocation of temporary or permanent network addresses to hosts.

IP requires the setting of many parameters within the protocol implementation software. Because IP can be used on many dissimilar kinds of network hardware, values for those parameters cannot be guessed at or assumed to have correct default values. The use of a distributed address allocation scheme based on a polling / defence mechanism, for discovery of network addresses already in use, cannot guarantee unique network addresses because hosts may not always be able to

defend their network addresses. DHCP supports three mechanisms for IP address allocation:

- 1. Automatic allocation : DHCP assigns a permanent IP address to the host.
- 2. Dynamic allocation : DHCP assigns an IP address for a limited period of time.
- 3. Manual allocation : The host's address is assigned by a network administrator.

DHCP is a draft standard protocol. Its status is elective. The current DHCP specifications can be found in *RFC 2131 – Dynamic Host Configuration Protocol* and *RFC 2132 – DHCP Options and BOOTP Vendor Extensions.*

Configuration Parameters Repository

DHCP provides persistent storage of network parameters for network clients. A DHCP Server stores a key-value entry for each client, the key being some unique identifier, for example an IP subnet number and a unique identifier within the subnet (normally a hardware address), and the value contains the configuration parameters last allocated to this particular client.

One effect of this is that a DHCP client will tend to always be allocated the same IP address by the server, provided the pool of addresses is not over-subscribed and the previous address has not already been allocated to another client.

DHCP Considerations

DHCP dynamic allocation of IP addresses and configuration parameters relieves the network administrator of great deal of manual configuration work. The ability for a device to be

moved from network to network and to automatically obtain valid configuration parameters for the current network can be of great benefit to mobile users. Also, because IP addresses are only allocated when clients are actually active, it is possible, by the use of reasonably short lease times and the fact that mobile clients do not need to be allocated more than one address, to reduce the total number of addresses in use in an organization. However, the following should be considered when DHCP is being implemented:

- DHCP is built on UDP, which is, as yet, inherently insecure. In normal operation, an unauthorized client could connect to a network and obtain a valid IP address and configuration. To prevent this, it is possible to preallocate IP addresses to particular MAC (Medium Access Control) addresses (similar to BOOTP), but this increases the administration workload and removes the benefit of recycling of addresses.

- Unauthorized DHCP Servers could also be set up, sending false and potentially disruptive information to clients.

- In a DHCP environment where automatic or dynamic address allocation is used, it is generally not possible to predetermine the IP address of a client at any particular point in time. In this case, if static DNS (Domain Name Server) servers are also used, the DNS servers will not likely contain valid host name to IP address mappings for the clients. If having client entries in the DNS is important for the network, one may use DHCP to manually assign IP addresses to those clients and then administer the client mappings in the DNS accordingly.

BOOTP and DHCP Inter operability

The format of DHCP messages is based on the format of BOOTP messages, which enables BOOTP and DHCP clients to interoperate in certain circumstances. Support for BOOTP clients at a DHCP Server must be configured by a system administrator, if required.

DYNAMIC DOMAIN NAME SYSTEM

In order to take advantage of DHCP, yet still to be able to locate any specific host by means of a meaningful label, such as its host name, the following extensions to the Domain Name System (DNS) are required:

- A method for the host name to address mapping entry for a client in the domain name server to be updated, once the client has obtained an address from a DHCP Server.

- A method for the reverse address to host name mapping to take place once the client obtains its address.

- Updates to the DNS to take effect immediately, without the need for intervention by an administrator.

- Updates to the DNS to be authenticated to prevent unauthorized hosts from accessing the network and to stop imposters from using an existing host name and remapping the address entry for the unsuspecting host to that of its own.

- A method for primary and secondary DNS servers to quickly forward and receive changes as entries are being updated dynamically by clients In short, a secure Dynamic Domain Name System (DDNS) is necessary.

In summary, in the DHCP and DDNS environment, DHCP provides a device with a valid IP address for the point at which it is attached to the network. DDNS provides a method of locating that device by its host name, no matter where that device happens to be attached to a network and what IP address it has been allocated.

More explanations about the domain presented in the above sections can be found in the following publications incorporated herewith by reference:

- TCP/IP Tutorial and Technical Overview by Martin W. Murhammer, Orcun Atakan, Stefan Bretz, Larry R. Pugh, Kazunari Suzuki, David H. Wood pushibed by IBM International Technical Support Organization.
- "Internet in a nutshell" by Valerie Quercia, published by O'Reilly, October 1997.
- Request For Comments (RFCs) from the Internet Engineering Task Force (IETF):
  - RFC 2131: Dynamic Host Configuration Protocol

PROBLEM

The problem is to detect and deny unauthorized Dynamic Host Configuration Protocol (DHCP) servers attached to an IP Network.

Within an IP network, when a DHCP Client needs to acquire configuration information such as an IP address (for instance when the DHCP Client is powered on), said DHCP Client usually broadcasts a request to retrieve said configuration information from a DHCP Server. The DHCP service is provided by one or a plurality of DHCP servers, in order to optimally adjust configuration parameters. Due to the nature of the DHCP

protocol which is based on UDP (User Datagram Protocol) BOOTP broadcast, any DHCP Server attached to the IP network can answer requests from DHCP Clients and can therefore provide DHCP Clients with configuration parameters. Each DHCP Client selects and uses the configuration parameters comprised within one of the answers received from the DHCP Servers (usually, the DHCP Client selects and uses the configuration parameters received from the "fastest" DHCP Server to answer).

Once a DHCP Client has retrieved the requested configuration information (including its IP address) from a DHCP Server, said DHCP Client then can use said configuration information to access resources within the IP network. For instance, a DHCP Client uses its IP address to access a WEB Server within the IP network.

Some access and security considerations are associated with the configuration information retrieved by DHCP Clients. For instance, the IP address retrieved and used by a DHCP Client, may be used by a WEB server to identify said DHCP Client. The WEB Server can then only answer the requests of the DHCP Client which has this specific IP address. The DHCP Client configured with said specific IP address is therefore able to retrieve information from said WEB Server (for instance confidential information). A DHCP Client configured with an IP address different from said specific IP address is not able to retrieve confidential information from said WEB Server.

The configuration information provided by the DHCP Servers located in the IP Network are defined for instance by a Network Administrator. When said configuration information are in error, the DHCP Clients have problems to access resources within the IP Network. For instance, a WEB Server may only accept requests sent by the DHCP Clients which have a valid IP address (that is an IP address comprised within a

list of IP addresses controled by the Network Administrator). If the IP address retrieved from a DHCP Server by a DHCP Client is incorrect (that is an IP address which is not comprised within the list of valid IP addresses), said WEB Server will reject the requests originated from said DHCP Client. Said DHCP Client will have access problems and will not be able to retrieve information from said WEB Server because the DHCP Server sent it an incorrect IP address.

Inversely, an incorrect IP address provided to a DHCP Client may enable said DHCP Client to access a WEB Server that it is not supposed to access. There is a security problem, because said DHCP Client may access confidential information it is not supposed to access.

Some DHCP Servers providing DHCP Clients with configuration information in error, may be attached to the IP Network. Said DHCP Servers are called "unauthorized DHCP Servers", or "invalid DHCP Servers", because they are not controled by a Network Administrator. Unauthorized DHCP Servers may be attached to the IP network for instance by inconscious people testing some DHCP functions, or by malicious people whose goal is to create access problems within the IP network. The problems are then to:

- Detect any unauthorized DHCP Server attached to the IP Network.

- Inhibit any unauthorized DHCP Server attached to the IP Network. The goal of this inhibition is
  - to avoid as much as possible unauthorized DHCP Servers to answer DHCP Clients requesting configuration information,
  - to reserve as many IP addresses as possible in the unauthorized DHCP Server so that said DHCP Servers runs

out of the IP addresses they can provide to the DHCP Clients.

- to minimize the number of DHCP Clients receiving configuration information in error by said unauthorized DHCP Servers, and
- to minimize the access problems caused by said unauthorized DHCP Servers.

Objects of the invention

- One object of the present invention is to detect unauthorized DHCP Servers.

- It is a further object of the present invention to neutralize unauthorized DHCP Servers.

- It is another object of the present invention to limit the impact of unauthorized DHCP servers within the IP network.

- It I yet another object of the present invention to reserve as many IP addresses as possible in the unauthorized DHCP Servers, so that said DHCP Servers runs out of their available IP addresses.

- It is yet another object of the present invention to improve the quality of the DHCP service.

Summary of the invention

The present invention relates to computer networks and in particular discloses a method and system, in a network device, for detecting and neutralizing o unauthorized Dynamic Host

Configuration Protocol (DHCP) servers in an Internet Protocol (IP) network. The method comprises the step of:

- simulating a plurality of clients, said step comprising the further steps of:
  - reserving in each unauthorized DHCP server as many IP addresses as possible, and/or
  - flooding each unauthorized DHCP server with a plurality of IP address renewal requests.

The step of reserving in each unauthorized DHCP server as many IP addresses as possible comprises the step of sending to each said unauthorized DHCP servers a plurality of different IP address requests.

The step of flooding each unauthorized DHCP server with a plurality of IP address renewal requests comprises the step of sending to each said unauthorized DHCP servers a plurality of different IP address renewal requests.

Drawings

The novel and inventive features believed characteristics of the invention are set forth in the appended claims. The invention itself, however, as well as a preferred mode of use, further objects and advantages thereof, will best be understood by reference to the following detailed description of an illustrative detailed embodiment when read in conjunction with the accompanying drawings, wherein :

- Figure 1 shows the allocation of an IP address to a DHCP Client by a DHCP Server according to prior art.

- Figure 2 is a view of a DHCP Checker Client according to the present invention.

- Figure 3 is a flow chart of an Invalid Server Detector according to the present invention.

- Figure 4 is a view of an Invalid Server Denial Handler according to the present invention.

Preferred embodiment of the invention

IP ADDRESS ALLOCATION

Figure 1 describes the DHCP Client/Server interactions when the DHCP Client does not know its network address. More particularly, Figure 1 shows the acquisition mechanism by a DHCP Client of the IP address and the IP minimal configuration parameters provided by a DHCP Server within an IP network. The DHCP Client (101) broadcasts a request on its local physical subnet (103). The request is forwarded by any router having a BOOTP forwarding mechanism. When the request is received by a DHCP Server (102), the DHCP Server checks whether it is able to answer the DHCP Client or not. If the DHCP Server has still some available IP address within its address database, a positive answer is returned to the DHCP Client. The DHCP Client selects the first DHCP Server for which a positive answer is received and confirms to this server its agreement.

More particularly the allocation of a new network address comprises the following steps:

- The DHCP Client broadcasts a request (a DHCPDISCOVER message) on its local physical subnet. The request may include some options such as network address suggestion or lease duration.

- Each DHCP Server may respond with a message (a DHCPOFFER message) that includes an available network address and other configuration options. The DHCP Server may record the address as offered to the DHCP Client to prevent the same address being offered to other DHCP Clients in the event of further messages being received before the first DHCP Client has completed its configuration.

- The DHCP Client receives one or more messages from one or more DHCP Servers. The DHCP Client chooses one based on the configuration parameters offered and broadcasts a message (a DHCPREQUEST message) that includes the DHCP Server identifier option to indicate which message it has selected and the requested IP address option, taken from the DHCP Client IP address in the selected offer.

- The DHCP Servers receive the messages broadcasted by the DHCP Client. Those DHCP Servers not selected use the message as notification that the DHCP Client has declined that DHCP Server's offer. The DHCP Server selected in the message commits the binding for the DHCP Client to persistent storage and responds with a message containing the configuration parameters for the requesting DHCP Client.

- The DHCP Client receives the message with configuration parameters and performs a final check on the parameters. At this point the DHCP Client is configured.

DHCP CHECKER CLIENT

The present invention relates to a system and method for detecting and neutralizing unauthorized DHCP Servers attached to the IP Network. Figure 2 is a view of a system which is

used for detecting and neutralizing unauthorized DHCP Servers according to the present invention.

The DHCP Clients (201) on the IP Network (202) retrieve their configuration information from the DHCP Servers (203) (204) attached to the IP Network. Some DHCP Servers (203) attached to the IP Network are authorized DHCP Servers controlled by a Network Administrator. Said authorized DHCP Servers provide valid configuration information to the DHCP Clients (201). One or multiple other DHCP Servers (204), also attached to the IP Network, are unauthorized DHCP Servers (also referred to as an invalid DHCP Server). They are not controlled by a Network Administrator and they provide invalid configuration information to the DHCP Clients (201). Such unauthorized DHCP Server may be attached to the IP network for instance by unconscious people testing some DHCP functions, or by malicious people whose goal is to create access problems within the IP network.

A DHCP Checker Client (205) is also attached to the IP Network, according to the present invention. The DHCP Checker Client is preferably a computer program which can run on any system (for instance a workstation) attached to the IP Network (202). The DHCP Checker Client (205) carries out the method for detecting and neutralizing one (or multiple) unauthorized DHCP Server (204).

The DHCP Checker Client comprises one DHCP Server table (206). Said DHCP Server table (206) (a flat file in a preferred embodiment) is created by the Network Administrator in charge of the IP Network. Said DHCP Server table comprises the list of authorized DHCP Servers. Each authorized DHCP Server (203) is preferably identified within the DHCP Server table by its IP address. When the DHCP Checker Client is started:

- (207) an ***Invalid Server Detector*** component periodically sent requests (209) to retrieve (210) configuration information from the DHCP Servers (203) (204) attached to the IP Network (202). The Invalid Server Detector detects one or multiple unauthorized DHCP Servers (204), using the DHCP Server table (206) and using the "server identifier" option comprised in the DHCPOFFER message returned (210) by the DHCP Servers to provide configuration information.

When one or multiple unauthorized DHCP Servers (204) are detected by the Invalid Server Detector component (207), the DHCP Checker Client automatically starts one component:

- (208) an ***Invalid Server Denial Handler*** component simulates multiple DHCP Clients. It sends (211) a large number of requests to each unauthorized DHCP Server (204) detected by the Invalid Server Detector component, for retrieving (212) configuration information. Said requests comprise DHCPDISCOVER and DHCPREQUEST unicast messages, and uses 'giaddr', 'chaddr', and 'ciaddr' fields of said messages. The number of said requests depends on the configuration of the DHCP Checker Client.

The Invalid Server Denial Handler simulates multiple DHCP Clients. Its goal is to:

- avoid as much as possible that unauthorized DHCP Servers (204) to answer DHCP Clients (201) requesting configuration information.
- minimize the number of DHCP Clients (201) receiving configuration information in error by said unauthorized DHCP Servers (204).

- minimize the access problems caused by said unauthorized DHCP Servers.

Said goal is achieved by sending a large number of requests (211) to each unauthorized DHCP Server (204), in order to:

- overload each said unauthorized DHCP Server with said requests and the corresponding answers (212).

- reserve a large number of IP addresses for the DHCP Checker Client. Said IP addresses are therefore no longer available for other DHCP Clients (201).

As a consequence, each said unauthorized DHCP Server (204):

- is too busy to answer (214) all requests which are sent (213) by DHCP Clients (201)
- runs out of the available IP addresses which can be provided to DHCP Clients (201).

The number of DHCP Clients which retrieve (214) configuration information from said unauthorized DHCP Servers is therefore minimized.

INVALID SERVER DETECTOR

The Invalid Server Detector component of the DHCP Checker Client is preferably a computer program. This component is in charge of:

- periodically retrieving configuration information from the DHCP Servers (203) (204) attached to the IP Network (202).
- detecting each unauthorized DHCP Servers (204), using:

- the DHCP Server table (206)
- the "server identifier" option comprised in the DHCPOFFER message returned (210) by the DHCP Servers and comprising the configuration information.

The Invalid Server Detector component immediately starts when the DHCP Checker Client starts.

Figure 3 is a flow chart which refers to the internal logic of the Invalid Server Detector component, according to the present invention. This component:

- (301) requests an IP address. The DHCP Checker Client behaves as a normal DHCP Client (201). It sends a DHCPDISCOVER message on the IP Network, in order to request configuration parameters (including an IP address) from a DHCP Server. The DHCPDISCOVER message is a broadcast message which is sent to any system attached to the IP Network.

- (302) waits DHCPOFFER messages. Each DHCP Server (203) (204) attached to the IP Network and and satisfying the DHCPDISCOVER request sent by the Invalid Server Detector, answers said request with one DHCPOFFER message. Said DHCPOFFER message comprises:

  - the configuration information (including the IP address) proposed by the DHCP Server.
  - the 'server identifier' option. Said 'server identifier' option comprises the address (the IP address) of said DHCP Server.

The time that waits the Invalid Server Detector in order to receive the DHCPOFFER message sent by each DHCP Server, is

preferably a configuration parameter of the DHCP Checker Client.

- (303) releases the IP address proposed by each DHCP Server. Authorized DHCP Servers (203) may have sent a DHCPOFFER to propose configuration parameters. The Invalid Server Detector therefore releases said proposed configuration parameters so that they can be used by normal DHCP Clients (201). In order to release the IP address proposed by each DHCP Server, the Invalid Server Detector sends a DHCPREQUEST broadcast message comprising:

  - The 'server identifier' option. Said option is not set by the Invalid Server Detector with the identifier of the DHCP Server which has been selected, but comprises the identifier (the IP address) of a DHCP Server which does not exist (for instance 10.1.1.1).

When each DHCP Server (203) (204) receives said DHCPREQUEST message, it compares the IP address comprised within the 'server identifier' option and its own IP address. Since the 'server identifier' and its IP address are different, said DHCP Server marks the proposed configuration parameters as being available again for other DHCP Clients.

- (304) builds a list (called "List_R") of the DHCP Servers which have sent a DHCPOFFER. Said list "List_R" comprises the IP address of each said DHCP Server. The list "List_R" is built using the 'server identifier' option comprised in each DHCPOFFER message received in (202). The IP address of each DHCP Server which has sent a DHCPOFFER is extracted from said 'server identifier' option.

- (305) retrieves a list (called "List_A") of all authorized DHCP Servers. This list is retrieved from the DHCP Server table (306). Said list "List_A" comprises the IP address of each authorized DHCP Server.

- (307) extracts from "List_R" a list (called "List_D") of the DHCP Servers which are not in "List_A". Said "List_D" therefore comprises the IP address of each unauthorized (also referred to as invalid) DHCP Server.

- (308) tests whether "List_D" is empty or not.

- If "List_D" is empty. This means that no unauthorized (invalid) DHCP Server has been detected.

  - (309) Possibly, stores an information indicating that no invalid DHCP Server has been detected. Said information can be for instance stored in a file located within the DHCP checker Client.

  - (310) exits the Invalid Server Detector. The DHCP Checker Client then starts again the Invalid Server Detector and with it the procedure for detecting unauthorized DHCP Servers (301). The time that waits the DHCP Checker Client to start again the Invalid Server Detector is preferably a configuration paramater of the DHCP Checker Client.

- If "List_D" is not empty. This means that one or multiple unauthorized (invalid) DHCP Servers have been detected.

  - (311) Possibly, stores an information indicating that one or multiple invalid DHCP Servers have been

detected. For instance, said information comprises the IP address of each said unauthorized DHCP Server, and is stored in a file located within the DHCP checker Client. An alert comprising said information is can also be sent to a Network Administrator. The Network Administrator can then (for instance) disconnect each unauthorized DHCP Server from the IP Network.

- (312) calls the Invalid Server Denial Handler.

INVALID SERVER DENIAL HANDLER

The Invalid Server Denial Handler component of the DHCP Checker Client is preferably a computer program. This component is in charge of:

- sending a large number of requests, for retrieving (212) configuration information, to each unauthorized DHCP Server (204) detected by the Invalid Server Detector component. Said requests comprise DHCPDISCOVER and DHCPREQUEST unicast messages, and uses the 'giaddr', 'chaddr', and 'ciaddr' fields of said messages. The number of said requests is a configuration parameter of the DHCP Checker Client.

The Invalid Server Denial Handler simulates multiple DHCP Clients. Its goal is to:

- avoid as much as possible that unauthorized DHCP Servers (204) answer DHCP Clients (201) requesting configuration information.
- minimize the number of DHCP Clients (201) which are provided configuration information in error by the unauthorized DHCP Servers (204).

- minimize the access problems caused by said unauthorized DHCP Servers.

Said goal is achieved by sending a large number of requests (211) to each unauthorized DHCP Server (204), in order to:

- overload each said unauthorized DHCP Server with said requests and the corresponding answers (212).

- reserve a large number of IP addresses for the DHCP Checker Client. Said IP addresses are therefore no longer available for other DHCP Clients (201).

As a consequence, each said unauthorized DHCP Server (204):

- is too busy to answer (214) all requests which are sent (213) by DHCP Clients (201)
- runs out of the available IP addresses which can be provided to DHCP Clients (201).

The number of DHCP Clients which retrieve (214) configuration information from said unauthorized DHCP Servers is therefore minimized.

The Invalid Server Denial Handler component is called by the Invalid Server Detector when one or multiple unauthorized (invalid) DHCP Servers have been detected. Figure 4 is a flow chart which refers to the internal logic of the Invalid Server Denial Handler component, according to the present invention. This component:

- (401) retrieves one DHCP Server from "List_D". "List_D" comprises the IP address of each unauthorized (invalid) DHCP

Server ("List_D" is built by the Invalid Server Detector). Said DHCP Server is therefore an unauthorized DHCP Server, and has to be processed by the Invalid Server Denial Handler.

- (402) tests if there is still one DHCP Server to process.

  - If there is no DHCP Server to process, this means that all unauthorized DHCP Servers detected by the Invalid Server Detector have been processed by the Invalid Server Denial Handler.

    - (403) exits the Invalid Server Denial Handler. The DHCP Checker Client then periodically starts again the Invalid Server Detector, and with it the procedure for detecting unauthorized DHCP Servers (301). The time that waits the DHCP Checker Client to start again the Invalid Server Detector is preferably a configuration parameter of the DHCP Checker Client.

  - If there is still one DHCP Server to process, this means that all unauthorized DHCP Servers detected by the Invalid Server Detector have not yet been processed by the Invalid Server Denial Handler.

    - (404) sends multiple DHCPREQUEST messages to said DHCP Server. The Invalid Server Denial Handler sends a large number of DHCPREQUEST messages to said specific DHCP Server. Said number is preferably a configuration parameter of the DHCP Checker Client (for instance 50 messages can be sent). Each said DHCPREQUEST message has the following characteristics:

- Each message is an **unicast** message which destination is said DHCP Server. Since the message is a unicast message, the traffic within the IP Network is minimized, and the impact of said traffic on the devices attached to the IP Network is minimized (as compared to a broadcast message sent to all devices attached to the IP network). For instance, the DHCP Clients attached to the IP Network do not have to waste time reading said unicast message (as opposed to a broadcast message, where each DHCP Client has to read the broadcast message just to determine that it does not have to answer it).

- The '**ciaddr**' field comprised in each said DHCPREQUEST is set by the Invalid Server Denial Handler with an IP address not comprised within the range of the valid addresses used within the IP Network. Said range of valid IP addresses is for instance a configuration information of the DHCP Checker Client, provided by a Network Administrator. Since the DHCP Server receives a DHCPREQUEST request comprising an invalid (and therefore unknown) IP address in the 'ciaddr" field, said DHCP Server takes some time to determine that it cannot satisfy said request. During said time, the DHCP Server is busy and therefore is usually not able to answer all the requests sent (213) by normal DHCP Clients (201).

- (405) sends multiple DHCPDISCOVER messages to said DHCP Server. The Invalid Server Denial Handler sends a large number of DHCPDISCOVER messages to said specific DHCP Server. Said number is preferably a configuration

parameter of the DHCP Checker Client (for instance 50 messages can be sent). Each DHCPDISCOVER message has the following characteristics:

- Each message is an **unicast** message which destination is said DHCP Server. Since each message is an unicast message, the traffic within the IP Network is minimized and the impact of said traffic on the devices attached to the IP Network is also minimized (as compared to a broadcast message which is sent to all devices attached to the IP network). For instance, the DHCP Clients attached to the IP Network do not have to waste time reading said unicast message (as opposed to a broadcast message, where each DHCP Client has to read the broadcase message just to determine that it does not have to answer it).

- The '**chaddr**' field comprised in each said DHCPDISCOVER is set by the Invalid Server Denial Handler with a MAC address which is:

  - not comprised within a range of valid MAC addresses used within the IP Network. Said MAC address is therefore unknown within the IP Network. Said range of valid MAC addresses is for instance a configuration information of the DHCP Checker Client provided by a Network Administrator.
  - not already used for another DHCPDISCOVER previously sent by the Invalid Server Denial Handler.

Since the DHCP Server receives a DHCPDISCOVER request comprising a new unknown MAC address in the 'chaddr" field, said DHCP Server reserves a new IP address for said MAC address. The IP address is reserved by the DHCP Checker Client. Said IP address is therefore no longer available and cannot be provided any more to the normal DHCP Clients (201) which may request (213) configuration parameters from said unauthorized DHCP Server.

The DHCP Server reserves one IP address for the DHCP Checker Client, for each DHCPDISCOVER message. Since a large number of DHCPDISCOVER messages are received by said DHCP Server, said DHCP Server finally runs out of the available IP addresses that can be provided to DHCP Clients (201).

- The **'giaddr'** field comprised in each said DHCPDISCOVER is set by the Invalid Server Denial Handler with the IP address of the DHCP Checker Client. Since the DHCP Server then receives a DHCPDISCOVER request comprising an IP address in the 'giaddr" field, said DHCP Server then answers said request with a DHCPOFFER message which destination is said IP address. The DHCP Checker Client is then able to receive the DHCPOFFER messages sent by the DHCP Server since the DHCP Checker Client is the destination of said messages.

- Optionnaly, the DHCPDISCOVER request also comprises the "IP address lease time" option set to request a very long lease time (for instance one week) or even an infinite lease time. In this case, the DHCP

Server may reserve for a very long time the IP address for the MAC address comprised in the 'chaddr' field of the DHCPDISCOVER request. Since said IP address is reserved for a very long period of time, the DHCP Server is then no longer able to provide said IP address to the normal DHCP Clients (201) during said long period of time.

- (406) waits for a message from the DHCP Server. Said message is for instance a DHCPOFFER message in response to a DHCPDISCOVER request. The time that waits the Invalid Server Denial Handler in order to receive said messages, is preferably a configuration parameter of the DHCP Checker Client.

- (407) tests whether there is a DHCPOFFER message to process or not.

  - If there is no DHCPOFFER message to process, then the denial of said DHCP Server is complete. Other unauthorized DHCP Servers may have to be denied. The Invalid Server Denial Handler loops to retrieve the next unauthorized DHCP Server to process.

    - (401) retrieves one DHCP Server from "List_D". "List_D" comprises the IP address of each unauthorized (invalid) DHCP Server. "List_D" is built by the Invalid Server Detector. Said DHCP Server is therefore an unauthorized DHCP Server, and has to be processed by the Invalid Server Denial Handler.

- If there is one DHCPOFFER message to process, this DHCPOFFER message is the answer to the DHCPDISCOVER message sent to the DHCP Server. Said DHCPOFFER message comprises the configuration information proposed by the DHCP Server (including the proposed IP address).

- (408) sends a DHCPREQUEST message to the DHCP Server. The Invalid Server Denial Handler sends a DHCPREQUEST unicast message to said specific DHCP Server, in order to accept the IP address proposed in the DHCPOFFER. Said DHCPREQUEST is built according to the DHCP protocol, using the information retrieved from the DHCPOFFER message. When the DHCP Server receives said DHCPREQUEST message, it definitively reserves the proposed IP address and this IP address cannot be allocated to another DHCP Client. The Invalid Server Denial Handler then loops back to (406) and waits for another message.

Note : The step of flooding each unauthorized DHCP server with a plurality of IP address renewal requests and the step of reserving in each unauthorized DHCP server as many IP addresses as possible can be implemented together in a same embodiment as described above or independently in distinct embodiments.

ADVANTAGES

The present inventions provides the following advantages:

- Unauthorized DHCP Servers are detected, and can for instance be physically removed from the IP Network by a Network Administrator.

- The negative effects generated by unauthorized DHCP Servers whithin the IP Network are limited. In particular, the number of DHCP Clients receiving configuration information from said unauthorized DHCP Servers is minimized. When the configuration information is in error, the number of DHCP Clients in error is therefore minimized.

- The traffic required within the IP Network for detecting and neutralizing unauthorized DHCP Servers is minimized. In particular, no broadcast message is used (only unicast messages are used) for the denial of unauthorized DHCP Servers. Because each device within the IP network has to read broadcast messages, said broadcast messages have usually a negative impact on the performance of said devices. For instance, a DHCP Client has to read each broadcast message, just to determine that it does not have to answer it. Since no broadcast message is used for neutralizing unauthorized DHCP Servers, the impact on the performance of each device attached to the IP Network is therefore minimized.

- The quality of the DHCP Service is improved because the impact within the IP network of the unauthorized DHCP Servers is limited. The number DHCP Clients configured with information in error is limited. Consequently, the number of access problems within the IP Network is also limited.

- The security within the IP Network is improved. Since the number of DHCP Clients in error is minimized, the risk of having DHCP Clients configured with information in error allowing access to confidential information is limited.

- No additional or specific hardware is required.

While the invention has been particularly shown and described with reference to a preferred embodiment, it will be understood that various changes in form and detail may be made therein without departing from the spirit, and scope of the invention.

Claims

1. A method, in a network device, for detecting and neutralizing unauthorized Dynamic Host Configuration Protocol (DHCP) servers (602) in an Internet Protocol (IP) network, said method comprising the steps of:

- simulating a plurality of clients, said step comprising the further steps of:

  - reserving (405) in each unauthorized DHCP server as many IP addresses as possible, and/or

  - flooding (404) each unauthorized DHCP server with a plurality of IP address renewal requests.

2. The method according to the preceding claim wherein the step of reserving in each unauthorized DHCP server as many IP addresses as possible comprises the steps of:

- simulating (405) to each unauthorized DHCP servers a plurality of clients requesting an IP address, said step comprising the step of:

  - sending to each said unauthorized DHCP servers a plurality of different IP address requests.

3. The method according to any one of the preceding claims wherein the step of flooding each unauthorized DHCP server

with a plurality of IP address renewal requests comprises the steps of:

- simulating (404) to each unauthorized DHCP servers a plurality of clients requesting the renewal of their IP address, said step comprising the step of:

  - sending to each said unauthorized DHCP servers a plurality of different IP address renewal requests.

4. The method according to any one of the preceding claims wherein each IP address renewal request comprises an unknown client IP address.

5. The method according to any one of the preceding claims wherein, in said step of sending to each said unauthorized DHCP servers a plurality of different IP address requests, each IP address request comprises an unknown client Medium Access Control (MAC) address and the IP address of the network device.

6. The method according to any one of the preceding claims comprising the preliminary steps of:

- simulating a client requesting an IP address, said step comprising the steps of

  - broadcasting (301) a request for an IP address over the IP network;

- receiving (302) one or a plurality of responses from respectively one or a plurality of DHCP servers;

- identifying (304) for each response the DHCP server that has originated the response;

- determining (307) for each identified DHCP server whether said identified DHCP server is authorized or not referring to a table (306), said table comprising a list of authorized DHCP servers.

7. The method according to any one of the preceding claims wherein said step of identifying (304) in each response the DHCP server that has originated the response comprises the step of:

- retrieving (302) from each response the IP address of the DHCP server that has originated the response.

8. The method according to any one of the preceding claims wherein said table comprises the IP address of each authorized DHCP servers.

9. The method according to any one of the preceding claims wherein each response comprises a proposed IP address, said step of determining (307) for each identified DHCP server whether said identified DHCP server is authorized or not referring to a table (306) comprising the further step of:

- releasing (303) in each identified DHCP server the proposed IP address.

10. The method according to any one of the preceding claims wherein said step of releasing (303) each proposed IP address comprises the step of:

- broadcasting to each identified DHCP server a release message comprising an IP address of an unknown DHCP server.

11. The method according to any one of the preceding claims wherein said method is executed at predefined or/and regular periods of time.

12. A system, in particular a network device, comprising means adapted for carrying out the method according to any one of claims 1 to 11.

13. A computer readable medium comprising instructions adapted for carrying out the method according to any one of steps 1 to 11.

METHOD AND SYSTEM FOR DETECTING AND NEUTRALIZING UNAUTHORIZED DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) SERVERS IN AN INTERNET PROTOCOL (IP) NETWORK

Abstract

The present invention relates to computer networks and in particular to a method and system, in a network device, for detecting and neutralizing unauthorized Dynamic Host Configuration Protocol (DHCP) servers (602) in an Internet Protocol (IP) network. The method comprises the step of:

- simulating a plurality of clients, said step comprising the further steps of:
  - reserving (405) in each unauthorized DHCP server as many IP addresses as possible, and/or
  - flooding (404) each unauthorized DHCP server with a plurality of IP address renewal requests.

The step of reserving in each unauthorized DHCP server as many IP addresses as possible comprises the step of sending to each said unauthorized DHCP servers a plurality of different IP address requests.

The step of flooding each unauthorized DHCP server with a plurality of IP address renewal requests comprises the step of sending to each said unauthorized DHCP servers a plurality of different IP address renewal requests.

Figure 2

IP Address Allocation

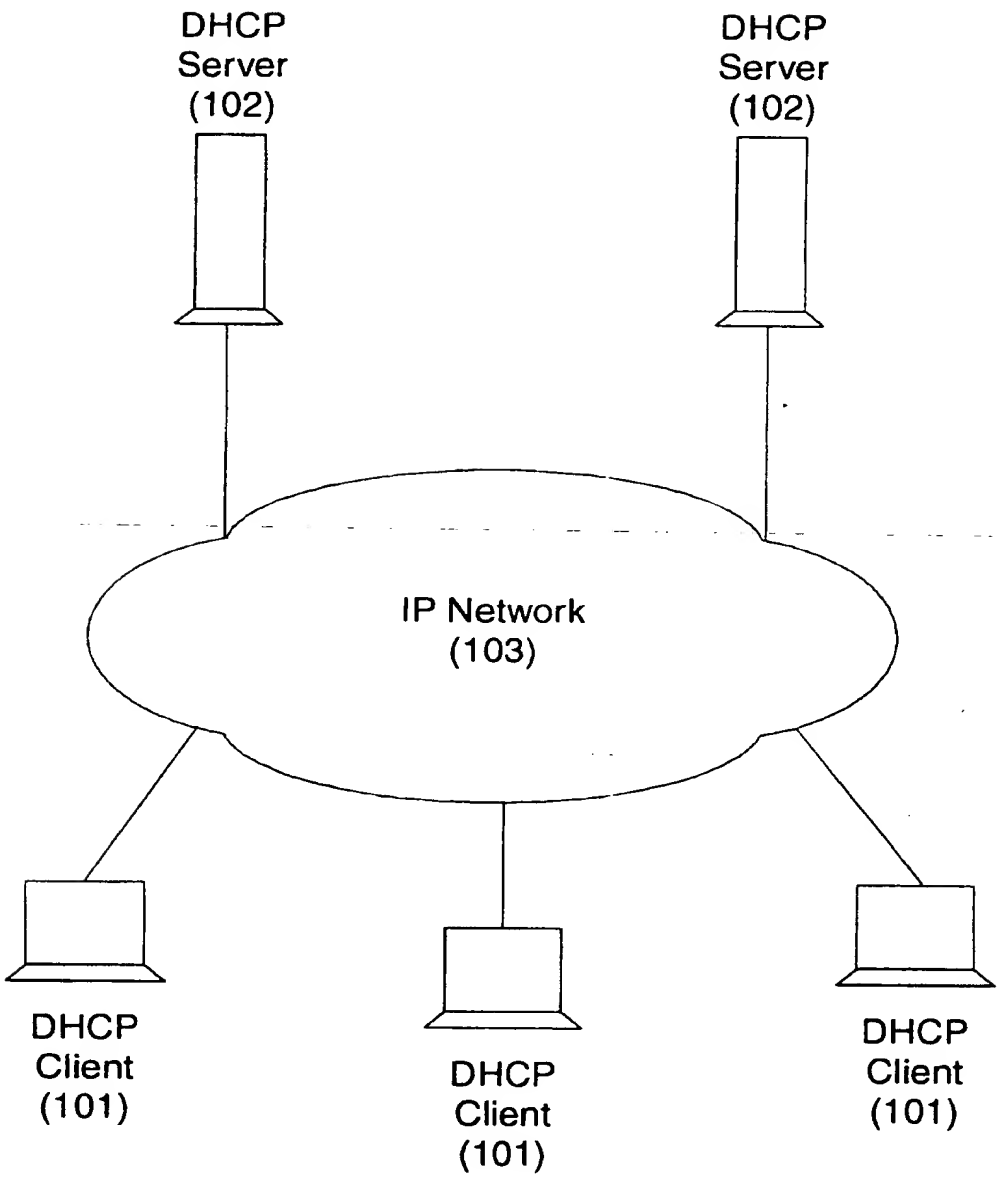

FIG. 1

View of the DHCP Checker Client

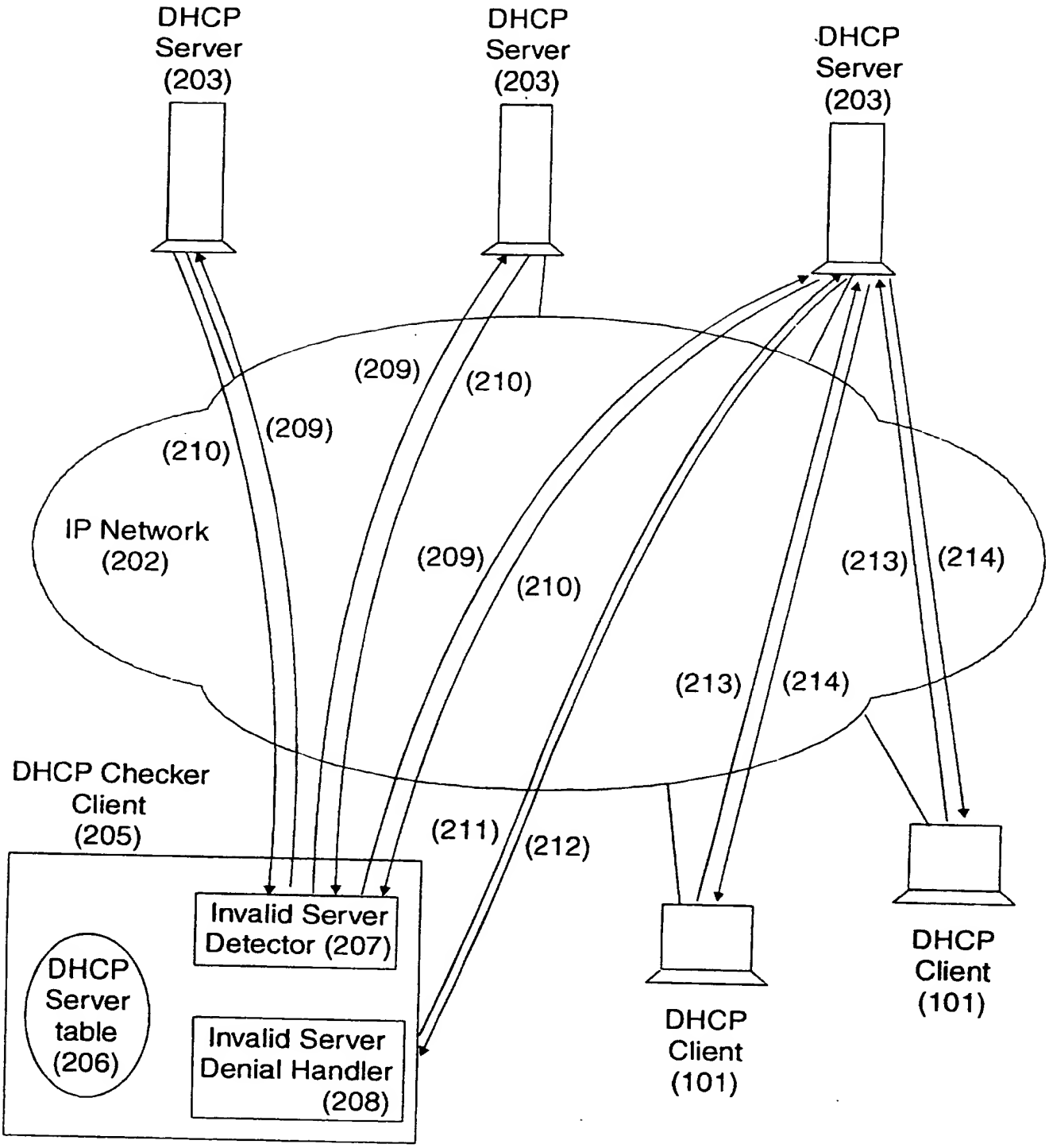

FIG. 2

Internal Flows of the Invalid Server Detector

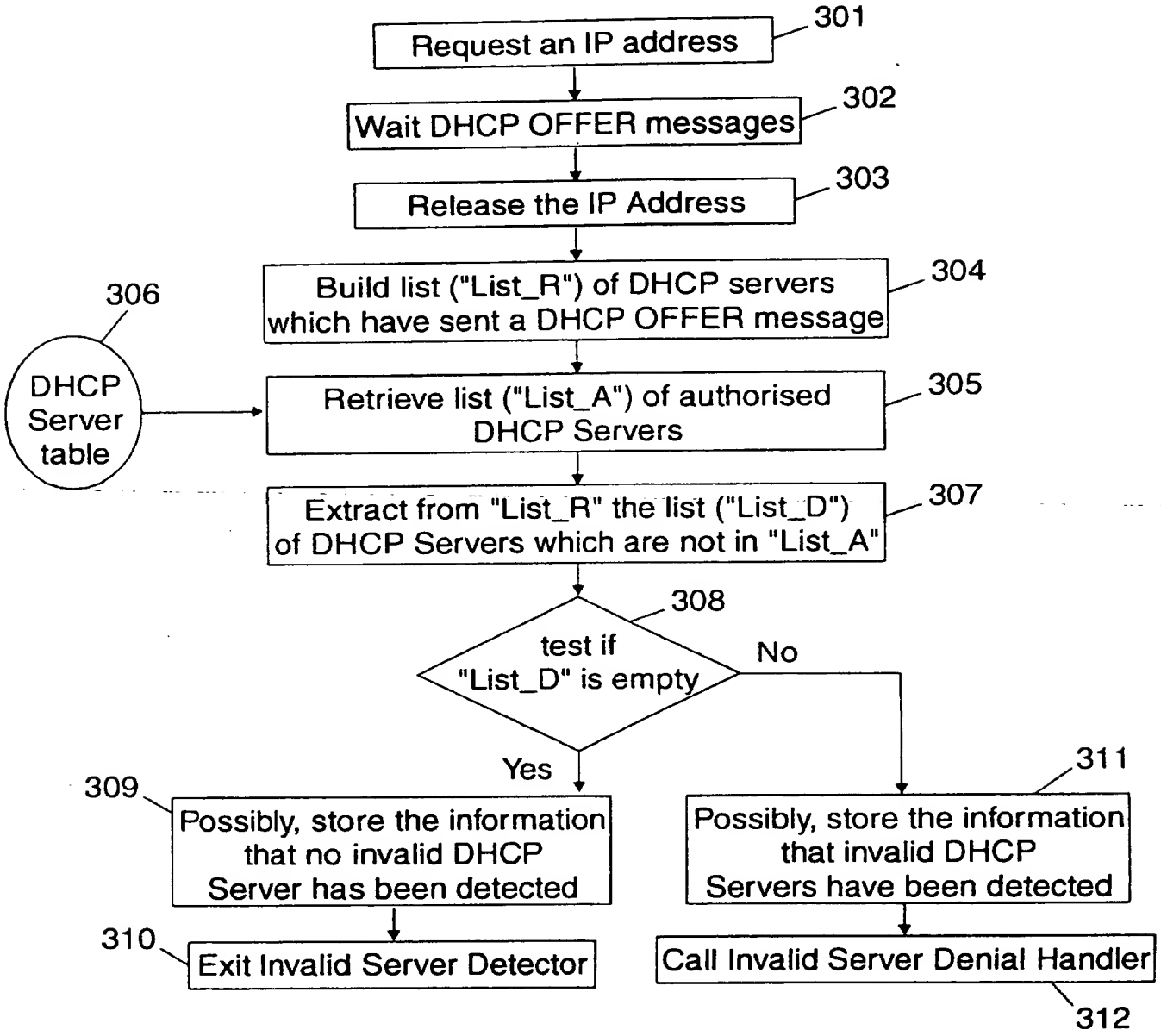

FIG. 3

Internal Flows of the Invalid Server Denial Handler

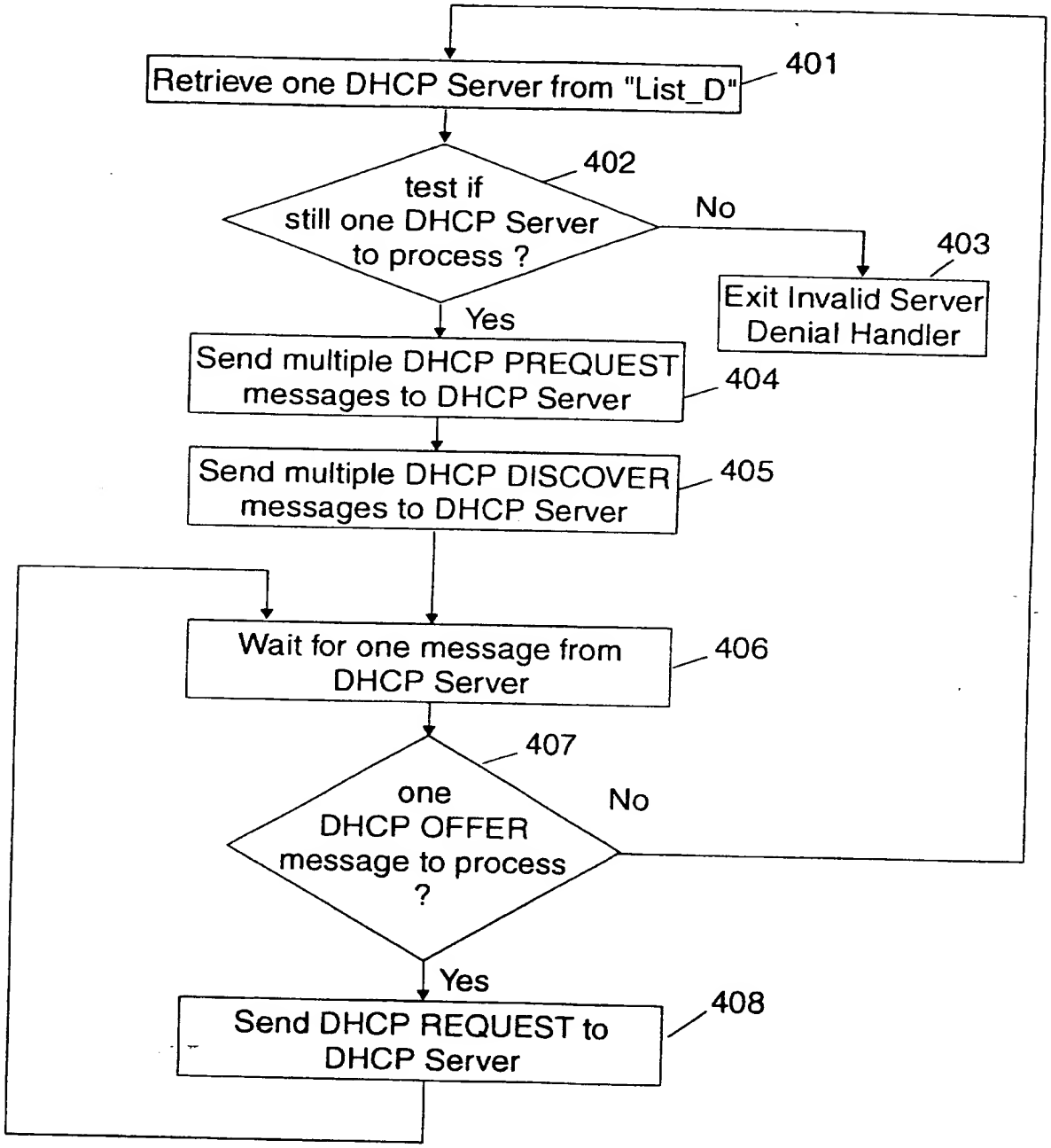

FIG. 4